





Preemptive Web Application & API Protection

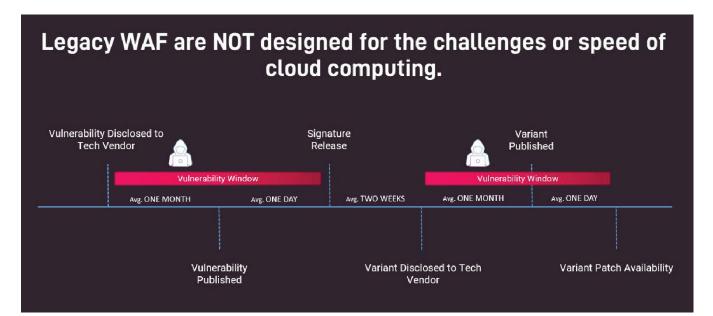
Don't Get Caught Off-Guard

As your cloud based web applications expand, so does your vulnerability to cyber threats. Attackers exploit your Web Applications and APIs using nefarious techniques like SQL injection, cross-site scripting and automated scripts a.k.a "bots." The fallout from such assaults can be highly detrimental and financially devastating, making application security an absolute priority for any business, big or small.

Traditional WAF Just Can't Cut It!

Web application firewalls (WAFs) have traditionally relied on threat signature mapping to reactively fend off attacks. This approach is both reactive (takes and avg of 1 month for initial rememdy) and is limited in its effectiveness because it can only make a binary decision: block or permit. This leads to a high number of false positives, causing headaches for security teams who must constantly monitor and maintain them.

With modern applications being developed and deployed at breakneck speed, it is becoming increasingly clear that this outdated approach is unable to keep up with the pace and scope of DevOps practices.





Eliminate Risks, Reduce Overheads, Accelerate Development

CloudGuard WAF is the ultimate solution for organizations looking to mitigate risks and speed up development. This advanced cloud native platform streamlines Application security management and re-imagines threat prevention, effectively blocking known and unknown threats and significantly reducing operational overheads.



Real-time Preemptive Protection

CloudGuard WAF preemptively blocks attacks, based on patented contextual AI/ML. WAF embeds security testing directly into the development pipeline, providing real-time protection. The result is enhanced security, accelerated time to-market, and greater development efficiency, all achieved without compromising on quality or safety.



Precise Prevention

CloudGuard WAF accurately eliminates false positives by examining various contextual parameters and determining a final risk score with input from multiple ML engines. Using multiple engine risk analysis provides more accurate decisionmaking eradicating manual tuning and enabling security admins to operate confidently in Prevent Mode without blocking legitimate requests.



Business Specific Protection

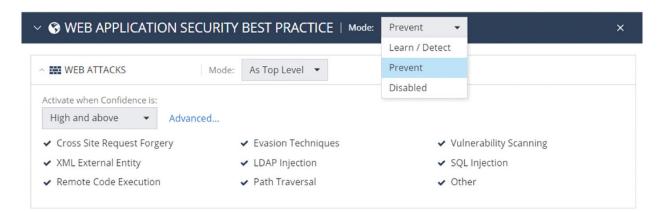
Web apps enter learning mode to gather environment-specific data and business cases, with multiple CPUs storing and synchronizing information hourly. Thesystem id entifies the source, HTTP method, HTTP requests, and every key/value pair, quickly completing its learning before users switch to prevent mode.

GENERAL

THREAT PREVENTION

BEHAVIORS E

EXCEPTIONS EVENTS





API Discovery

Applications are evolving faster than ever and as they do, they create and expose more APIs. Ensure that your application's APIs are being used correctly, with CloudGuard WAF's API discovery, as well as auto generated OpenAPI SWAGGER schema files. Stop cyber criminals from leveraging your APIs to expose sensitive data, inject commands or to extract API keys.

Prevent Automated Attacks

Protect your applications from sophisticated bots. CloudGuard uses JS injections to perform clientside behavioral analysis (including biometric activity like key strokes and mouse movements), in order to distinguish between human and non-human interactions with your application. Stop credential stuffing, brute force attacks and site scraping with advanced bot protection.

🛛 🕲 Olejects 🔹 🖉 Install Policy													
Logs General Overview >	New Tab +											Q. Search	
* Gueries @ Q @ All	Time . Enter secon	th query (Ctrl+P)											
											Query Syntax	Object Categories	
4 Canada Oranian	Contrast associate	Tomas Nations and a	the malles								Options		
 General Overview > Critical Attack Types Not prevented by policy 											Options	Services	
Attack Types by Blades						Activity Timeline						# Applications/Categories	
						Critical Children						VPN Communities	
7 IPS		Anti-Bot	1	2 Threat								de Outs lipes	
				Emula	ition							424 Users	
						lage						C Time Objects	
Anti Mar			tector	•• 0 Three	Extraction							X UserCheck Interactions	
🛛 😵 3 Anti-Viru	~ V	0 DDoS Pro	lector [0	C EXCIDENCION							🔁 Linit	
						Feb 13, 201	1:00 AM	1:00 AM 1:00	AM 1:00 AM	Dec 10, 2019 Ref	6 8, 2020		
					Top Attacks								
Top Attacks			Π.	Top Sources				Top Destinations					
Top Attacks	Country	: Blada	_	Top Sources	Countility	* Bute	Lees	Top Destinations	Severity	v Bala	Inter		
Protection Name		Blade	L	Source	Severity	• Bade	Logs S7	Destination		 Bade Threat Environ 	Logs		
Protection Name MIT Kerberos kadmind RPC		🔮 iPS	L 100	Source	Severity Critical	🍓 Multiple Blades	\$7 ×	Destination	Severity Critical	C Threat Emulation	12		
Protection Name	Critical	1	L 100 11	Source	Critical			Destination	Critical				
Protection Name MIT Kerberos kadmind RPC Backdoor/Win32/TaidoorA	Critical	🗊 195 🐨 Anti-Bot	L 100 11 8	Source 10 10/132.5.65 102.168.9.78	Critical Critical	 Multiple Bades IPS 	57 * 25	Destination 10.226.111.43 10.225.243.132	Critical	Threat Enviration IPS	12 10		
Protection Name MIT Kerberos Ladmind RPC Backdoor Win32Taidoor A Microsoft Windows RASMA	Criscal Criscal Criscal	195 19 Anti-Bot 11 IPS	L 100 11 8 6	Source 10 10.132.5.65 10 10.132.5.65 10 10.132.5.50	Critical Critical Critical	 Multiple Blades IPS Threat Emulation 	57 ^ 25 12	Destination 10.226.111.43 10.225.343.132 10.225.343.132 10.225.343.132	Critical Critical Critical	Threat Emulation IPS IPS	12 10		
Protection Name MIT Kerberos Ladmind RPC Backdoor/Win22/Taidoor A Microsoft Windows RASMA Exploited pdf document	Critical Critical Critical Critical	IPS Anti-Bot IPS IPS Dreat Emulation	L 100 11 8 6 6	Source 100 10.132.5.65 100 102.168.9.78 100 103.2.5.50 10.226.111.7	Critical Critical Critical Critical	Multiple Bades IPS Threat Environ IPS	57 * 25 12 10	Destination 10.226.111.43 10.225.243.192 102.168.72.71 192.168.72.40	Critical Critical Critical Critical	Threat Emulation FIPS FIP FIP	12 10		
Protection Name MIT Kerbens Ladmind RPC Backdoor/Win32/TadoonA Microsoft Windows RASMA Exploited pdf document Exploited doc document	Critical Critical Critical Critical Critical Critical	IPS Anti-Bot IPS Dreat Emulation Threat Emulation	L 1009 111 8 6 6 2	Source 50 10.132.5.65 102.168.9.78 50 10.132.5.50 10.226.111.7 50 10.132.5.218	Critical Critical Critical Critical Critical	 Multiple Bades IPS Theat Environ IPS IPS IPS 	57 * 25 12 10 6	Destination 10.226.111.49 10.225.343.192 10.225.343.192 10.255.468.72.71 10.198.168.72.40 10.7.98.85	Critical Critical Critical Critical Critical	Threat Emulation PS PS PS PS PS PS	12 10		
Protection Name MIT Karbenos kadmind RPC Backdoox/Wind2nadfAcodow Microsoft Windows RASMA Exploited polf document Exploited doc document Malicious Einary.balmbj	Critical Critical Critical Critical Critical Critical Critical	IPS Anti-Dot IPS Threat Envolution Threat Envolution Anti-Vinus	Lun 100 11 8 6 6 6 2 1	Source 10:132.5.65 10:132.5.65 10:132.5.50 10:132.5.20 10:132.5.218 10:132.5.218 10:132.5.28	Critical Critical Critical Critical Critical Critical	Multiple Blades IPS Threat Environ IPS IPS IPS IPS	57 * 25 12 10 6	Destination 10.226.111.48 10.226.343.102 10.226.343.102 10.286.343.102 10.286.85 10.798.85 10.798.85	Critical Critical Critical Critical Critical Critical	Threat Environ PS PS PS PS PS PS PS	12 10		
Protection Name MIT Kerberes Ladmind RPC Backdoor Win32/Taidoor A Microsoft Windows RADMAL Exploited doc document Exploited doc document Microsoft Windows Remote	Critical Critical Critical Critical Critical Critical Critical Critical	IPS Ansi-Bot IPS IPS D Threat Emulation Ansi-Virus IPS IPS	L 100 11 8 6 6 6 2 1 3 7	Source 50 10.132.5.65 10.132.5.65 10.132.5.50 10.226.111.7 10.132.5.218 10.132.5.218 10.132.5.218 10.132.5.101	Critical Critical Critical Critical Critical Critical Critical	 Multiple Bades IPS Threat Environ IPS IPS IPS IPS IPS IPS IPS 	57 ^ 25 12 10 6 5 4	Destination 10.226.111.43 10.225.243.132 10.125.243.132 10.125.243.132 10.125.243.132 10.125.243.132 10.125.243.132 10.125.243.132 10.136.85 10.136.85 10.136.82 10.136.82 10.136.84	Critical Critical Critical Critical Critical Critical Critical Critical	Prest Envirtion PS	12 10		
Protection Name MIT Generals Ladmind RPC Backdoor Windows RADMA Exploited pol document Exploited doc document Maloice Brany Jointhy Microsoft Windows Remote Arbit Technologies Security	Critical Critical Critical Critical Critical Critical Critical Critical High	IPS Anti-Bot IPS IPS Threat Emulation Anti-Vrus IPS IPS IPS	L 100 11 8 6 6 6 2 1 7 7 6	Source Source 10,132,5,65 10,206,9,78 10,226,111,7 10,226,111,7 10,132,5,218 10,132,5,218 10,132,5,101 10,132,5,101 10,132,5,101 10,132,5,101 10,132,5,101 10,132,5,101 10,132,5,101 10,132,5,101 10,132,5,101 10,132,5,5,5 10,132,5,5 10,132,5,5 10,132,5,5 10,132,5,5 10,132,5,5 10,23,5 10,13,5 10	Critical Critical Critical Critical Critical Critical Critical Critical	 Muttiple Blades PS Threat Environ PS PS	57 × 25 12 10 6 5 4 4 4	Destination 10.226.111.43 10.225.431.92 10.226.141.43 10.226.441.92 10.226.441.92 10.226.46.72.71 10.226.46.72.40 10.226.46.72.40 10.798.85 10.798.85 10.798.85 10.798.85 10.292.447 10.82.92.147	Critical Critical Critical Critical Critical Critical Critical Critical Critical Critical	Threat Emulation PS	12 10		
Protection Name MIT technical kalorinid RPC Backdoor,Win22.TashoosA Microsoft Windows RASMA. Exploited doc document Malicioa, Erony Jahimbij Microsoft Windows Remota Alsh-N Technologie Security- Novell advectory HTTP Hea.	Critical Critical Critical Critical Critical Critical Critical Critical High	PS Anti-Bot PS Anti-Bot PS Prest Emulation Anti-Virus PS PS PS PS	L 100 11 8 6 6 6 7 1 7 6 6	Source Source	Critical Critical Critical Critical Critical Critical Critical Critical Critical	 Multiple Blades IPS Threat Environ PS IPS 	57 A 25 12 10 6 5 4 4 4 4	Destination 10.226.111.48 10.225.343.192 10.253.343.192 10.253.343.192 10.253.343.192 10.253.343.192 10.253.343.192 10.253.254.192 10.2163.226.147 10.2163.264.192 10.2163.206.192 10.2166.206.206 10.2166.206 10.2166	Criscal Criscal Criscal Criscal Criscal Criscal Criscal Criscal Criscal	Prest Emulation PS	12 10		
Protection Name MIT Centeries Ladimid RPC – Backdoor/Win32Tastoor/A Microsoft Window RAMMA, Exploited poll document Exploited doc document Malorea Enary balmbj Microsoft Window Remetra, Art-N Technologies Senarty- Novel advectory HTTP Hea. Microsoft WING Local Prole.	Cristal Cristal Cristal Cristal Cristal Cristal Cristal High High High High	IPS Anti-Bot IPS IPS IPS IPS IPS Threat Emulation Threat Emulation Anti-Virus IPS IPS IPS IPS IPS IPS	L 100 111 8 6 6 6 7 1 7 6 6 6 4	Source 20 10 123.5.65 10 10 123.5.65 10 10 123.5.10 10 10 123.5.10 10 10 123.5.10 10 10 123.5.10 10 10 123.5.10 10 10 123.5.10 10 123.5.21 10 123.5.2 10 10 123.5.2 10 10 123.5.2	Critical Oritical Oritical Oritical Oritical Oritical Oritical Oritical Oritical	 Muttple Blades IPS Threat Environ PS IPS IPS<td>57 A 25 12 10 6 5 4 4 4 4</td><td>Destination III 0.226.111.48 III 0.225.443.192 III 0.225.443.192 III 0.215.443.192 III 0.215.443.192 III 0.215.443.192 III 0.215.443.192 III 0.215.453 III 0.215.457.190 III 10.215.457 III 10.215.457 III 10.215.457 III 10.215.427 III 10.215.427 III 10.216.20.02 III 10.2147.5</td><td>Chical Chical Chical Chical Chical Chical Chical Chical Chical Chical Chical</td><td>Dreat Emulation P5 P5</td><td>12 10</td><td></td><td></td>	57 A 25 12 10 6 5 4 4 4 4	Destination III 0.226.111.48 III 0.225.443.192 III 0.225.443.192 III 0.215.443.192 III 0.215.443.192 III 0.215.443.192 III 0.215.443.192 III 0.215.453 III 0.215.457.190 III 10.215.457 III 10.215.457 III 10.215.457 III 10.215.427 III 10.215.427 III 10.216.20.02 III 10.2147.5	Chical Chical Chical Chical Chical Chical Chical Chical Chical Chical Chical	Dreat Emulation P5	12 10		
Partection Name MIT Kerbers kadmind RPC – Beddees Win22 Madewah Morosoft Windows RADMA. Exploited doc document Exploited doc document Malocos Branybainelij Morosoft Windows Remote – Arbit Technologies Semity- Namit Boreccop HTD Hea. Morosoft Windows Hennite – DicAR-Technice Invisio	Cristal Cristal Cristal Cristal Cristal Cristal Cristal High High High High High	(175 (175	Lue 1000 113 8 6 6 2 1 1 7 6 6 6 6 4 4 4	Source 20 10:132.5.55 10 192.148.9.79 10 10:132.5.50 10 10:132.5.10 10 10:132.5.10 10 10:132.5.10 10 10:132.5.10 10 10:132.5.10 10 10:132.5.10 10 10:132.5.42 10 10:152.5.42 10 10 10:152.5.42 10 10:152.5.52 10 10:152.55 10 10 10:152.55 10 10 10:152.55	Critical Critical Critical Critical Critical Critical Critical Critical Critical Critical Critical	Image: Second	57 × 12 12 10 6 3 4 4 4 4 4 2	Cestination 10225-111-63 10225-111-63 10225-143-132 104 92-168-72-71 104 192-168-72-109 104 104-72-109 105-168-72-109 105-168-72-109 105-168-72-109 105-168-72-87 105-168-72-88 105-168-72-88 105-168-72-168 105-168 10	Criscal Criscal Criscal Criscal Criscal Criscal Criscal Criscal Criscal Criscal Criscal Criscal	Threat Environment Provide the second seco	12 10		
Protection Rome MIT Serbers Ladmid RPC – Rediden Wirk2.Tedesch Lipbister pill disconnet Esplotted dar document Mationa Branzhalmity Morsont Wirdsen Romote – Arb V Technologies Senarby– Norell elivenzity INTE Hea. Microsoft Wird Jocal Initia UCLAR-INET-IN UCLAR-INET-IN	Cristal Cristal Cristal Cristal Cristal Cristal Cristal High High High High High	PS Anti-bat PS Anti-bat PS Thest finalition Anti-Vins PS PS PS PS Anti-Vins PS Anti-Vins Anti-Vins Anti-Vins Anti-Vins Anti-Vins Anti-Vins	L 1009 111 8 6 6 7 7 8 6 6 4 4 4 3	Source Company States	Critical Critical Critical Critical Critical Critical Critical Critical Critical Critical Critical Critical	Image: Comparison Image: Comparison Image: Comparison Image: Comparison <td>57 × 12 12 10 6 3 4 4 4 4 4 2</td> <td>Cestination 10224.1143 2023.44.132 20125.44.132 20125.46.7241 20129.46.7240 20129.46.7240 20129.46.7240 20129.46.7240 20129.46.7240 20129.47.32</td> <td>Criscal Criscal Criscal Criscal Criscal Criscal Criscal Criscal Criscal Criscal Criscal</td> <td>C Threat Environ U IPS U</td> <td>12 10</td> <td></td> <td></td>	57 × 12 12 10 6 3 4 4 4 4 4 2	Cestination 10224.1143 2023.44.132 20125.44.132 20125.46.7241 20129.46.7240 20129.46.7240 20129.46.7240 20129.46.7240 20129.46.7240 20129.47.32	Criscal Criscal Criscal Criscal Criscal Criscal Criscal Criscal Criscal Criscal Criscal	C Threat Environ U IPS U	12 10		
Partection Nome MIT Generals Ladinical RPC Belidour Win22.ZaulouxA Microsoft Windows RobMak Esploited doc document Mallonas Branzybalmbj Microsoft Windows Remote Alch-1 Stechologer Security- Novell adorectory HTTP Hea. Microsoft WING (scall Hindie- DCAR-Tes File VisuaWIN21.East-Madifed Molipie Vendor StMMy H.	Critical Critical Critical Critical Critical Critical Critical Critical High High High High High	175 2 Ant-Set 2 Ant-Set 17 S 2 Ant-Set 17 S 17 Ant-Set 17 Ant-Set 17 Ant-Set 17 Ant-Set 17 S 17 Ant-Set 17 S 17 Ant-Set 17 S 17 Ant-Set 17 S 17 Ant-Set 17	L 1009 111 8 6 6 7 7 6 6 6 4 4 4 1	Secure 20 10.122.545 30 102.146.5.78 30 102.146.5.78 40 1022.61.1.7 30 101.25.5.01 30 101.25.5.10 30 101.25.5.10 30 101.25.5.10 30 101.25.5.42 30 102.5.92.4 40 102.5.4.11.8 40 102.5.4.11.8 40 102.5.5.6 40 102.5.5.6 40 102.5.5.6 40 102.5.5.6	Critical Critical Critical Critical Critical Critical Critical Critical Critical Critical Critical Critical Critical	№ Autype Traces № PS № Provide Travelation № PS	57 A 25 12 10 6 5 4 4 4 4 4 2 2 1	Castadian 10225.1143 2025.144392 2025.444392 20125.4467240 201294.85 201294.85 201294.85 201294.75 20	Criscal Criscal Criscal Criscal Criscal Criscal Criscal Criscal Criscal Criscal Criscal Criscal Criscal Criscal	♥ Threat Enviation ♥ P5	12 10 10 8 8 7 6 6 6 6 6 6 6 4 4 4		

AUTOMATED WEB APPLICATION AND API PROTECTION (WAF)

- Web Application Protection
- API Security
- Bot Prevention
- Intrusion Prevention (IPS)
- File Security

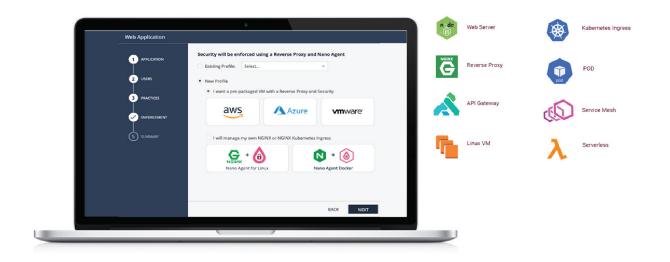
KEY PRODUCT BENEFITS

- Preemptive Protection: Contextual machine learning provides preciseanalysis, preventing known and unknown cyber attacks
- **CI/CD Automation:** Auto-deploy on any cloud, hands-off management, DevOps friendly by design
- **Utmost Efficiency:** No Signiture Update, No False Positives, No Manual Tuning



Cloud Distributed WAF

CloudGuard WAF can be deployed across various platforms including on-premises, agents, gateways, and SaaS. Our team is dedicatedly engaged in regularly enhancing and expanding our support for both widely adopted and cutting-edge technologies.



SUPPORTED ENVIRONMENTS

CLOUD

- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure
- VMware

CONTAINERS

- Docker
- Kubernetes
- Kubernetes Ingress

CPU'S

• X86 (64 bit)

OPERATING SYSTEMS

- CentOS
- Debian
- Red Hat Enterprise Linux
- Ubuntu

PROTECTION CATEGORIES

- Cross Site Request Forgery
- XML External Entity
- Remote Code Execution
- Evasion Techniques
- LDAP Injection
- Path Traversal
- Vulnerability Scanning
- SQL Injection
- Illegal HTTP Methods Invalid input to forms

and APIs Bot Scraping and Brute Force Attacks

• Over 2800 Web Specific CVEs



Dec 2022 - CloudGuard WAF Recognized as the Only WAF to successfully block a penetration test by Team82

Claroty Team82 has developed a generic bypass for web application firewalls (WAF). Major WAF products including: AWS, F5, CloudFlare, Imperva and Palo Alto were found to be vulnerable. CloudGuardd WAF pre-emptively blocked the attack/bypass, within seconds.





CLOUDGUARD NAMED LEADER IN GIGAOM 2024 RADAR REPORT FOR APPLICATION AND API SECURITY FOR 2 YEARS IN A ROW

"The biggest strength of the CloudGuard WAF solution is API protection. While All Vendors can either import or detect APIs and most vendors can do both, CloudGuard is able to do both and generate sample protection rules based upon the definition and information gleaned from traffic. This earned them our highest score on the API import and discovery key feature."

Don Mcvittie, Analyst | GigaOm





Worldwide Headquarters

5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters

100 Oracle Parkway, Suite 800, Redwood City, CA 94065 | Tel: 1-800-429-4391

www.checkpoint.com

© 2024 Check Point Software Technologies Ltd. All rights reserved.